Testimony of

Richard E. Hovel
Senior Aviation & Homeland Security Advisor
The Boeing Company

Before the House Homeland Security Committee
Subcommittee on Intelligence, Information Sharing,
and Terrorism Risk
Assessment

July 26, 2007

The US Department of Homeland Security has defined the concept of a fusion center as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, and respond to criminal, terrorist and other activity as affects our Critical Infrastructure Key Resources (CI/KR). To meet this challenge, fusion centers are evolving to an **all-threats, all-crimes, all-hazards** approach. Their intended function is to compile, blend, analyze, and disseminate information of various types such as Criminal Intelligence, Threat Assessments, Public Safety, Law Enforcement, Public Health and Social Services, to name a few. To establish this successfully, a "bottom up" approach is necessary, integrating information requirements of the private sector to form the program foundation. Once accomplished, measurable progress will be dependent upon mutually understood expectations, capitalizing on already-existing relationships between the public and private sector partners.

According to the recently released National Intelligence Estimate (NIE), the ability to detect broader and more diverse terrorist plots in our current environment is certain to challenge existing US defensive efforts, as well as the tools we use to detect and disrupt these plots. To meet this challenge will require a greater understanding of how suspect activities at the local level relate to strategic threat information, and how best to identify indicators of terrorist and other criminal activity in the midst of legitimate interactions. The private sector can offer fusion centers a variety of resources, including industry-specific subject-matter experts who can provide expertise when threats have been identified. This could include information pertinent to cyber crimes, risk assessments, suspicious incidents and activities, as well as information relative to the location of CI/KR. However, understanding and responding to the myriad of CI/KR **interdependencies** as well as **preparedness gaps** that exist between them, depends upon having the latest and most complete information available. Similarly, success in the public sector in these extremely sensitive areas is predicated on a thorough understanding of the far-reaching damage that a successful attack on CI/KR could have. Industry, as a whole, is acutely aware of the vital role one element may have in the successful continuity of operations of other elements. Because of the difference and complex nature of each element of the CI, as well as their already stated interdependencies, access to **all**

information both classified and unclassified, which potentially or actually threatens them, is vital.

One of the fundamental principals of fusion center partners should be the identification and sharing of terrorism-related leads, that is, any **nexus** between crime-related and other information collected by state, local, tribal and private sector entities suggesting the presence of a terrorist organization and/or likelihood of an attack. A clear understanding of the links between terrorism-related intelligence and terrorism-related information, e.g. flight training school, drug trafficking, etc, must be understood so as to identify those activities or events that are precursors or indicators of an emerging threat. It is essential that a partnership between public and private sector officials be solidified, so public sector representatives may become much more familiar with prevailing vulnerabilities and consequences in the private sector, of possible terrorist attacks. Likewise, the private sector must be better educated to the methods likely utilized by terrorist organizations, and the equipment and substances needed/used to carry out an attack with associated planning activities. An outreach to non-government experts in academia and the Private sector can also add the advantage of alternative analyses and new analytic tools to broaden and deepen the intelligence community's perspective.

Other information necessary, both classified and unclassified that is vital to the private sector is that which is **threat-specific, indicative of a long-term threat and tactics and methods** used by terrorist organizations to perpetrate an attack. One objective is the production of value-added intelligence products than can support the development of performance-driven, risk-based prevention, response and consequence management programs that will support specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages. Benefits of this will be realized in the improved flow of information from a common operating picture, which supports private sector resiliency while satisfying public sector mission requirements. More specific information needs attendant to individual elements of the CI/KR may best be the product of Key Resource Sector Councils, the American Society for Industrial Security (ASIS) or other OSAC-like groups that can speak to the more in-depth characteristics of each element.

On a related note, Boeing would like to thank Congress for passing the Critical Infrastructure Information Act of 2002. We are also pleased with the Final Rule issued by the Department of Homeland Security (DHS) on Procedures for Handling Critical Infrastructure Information, on September 1, 2006, in response to that Act.

This law encourages the private sector to voluntarily share security-related information about critical infrastructure by providing special protection for that information. Going forward it is extremely important for the public and private sector to work together to protect our national security, economy, and public welfare.

The type of information that Boeing provides includes assessment of the vulnerabilities of our aviation infrastructure, which includes our airplanes. Boeing believes that this information and the thorough risk management analysis that TSA and Boeing are

working on with others in government and industry are critical to improving security, safety and efficiency in U.S. commercial aviation. The U.S. aviation infrastructure remains a potential target for future terrorist strikes and the government and private sector need to keep a collective watchful eye. The PCII protections are essential to this work.

According to the NIE, al Qaeda's homeland plotting is likely to continue to focus on prominent political, economic and infrastructure targets with the goals of producing mass casualties, visually dramatic destruction, significant economic aftershocks and/or fear among the US population. It goes without saying that al Qaeda will continue to try to acquire and employ weapons of mass destruction (WMD) and would not hesitate to use them if it develops what it deems is sufficient capability. There are increasingly aggressive internet sites espousing anti-US rhetoric and actions, and a growing number of radical, self-generating cells in Western countries, indicating that the radical and violent segment of the West's Muslim population is expanding within the US. Other non-Muslim terrorist groups will also most likely conduct attacks over the next three years given their violent histories. To date, the bulk of the deadly attacks experienced, have been directed toward the private and quasi-private sectors. The loss of lives and damage to property suffered both domestically and overseas has been astronomical, giving companies a vested interest in joining in the fight. Currently, the resources of the private sector are hardly being tapped. Instead for the most part, businesses are (still) sitting on the sidelines relying on the US government for protection. This not only weakens our ability to eliminate terrorism, but it overlooks the fact that this is a shared problem that involves us all. The chance of winning the fight against terrorism exists, but we all need to contribute to the solution – a solution that necessitates expansion of the intelligence gathering role beyond its limits to date, and overcoming the crippling attitude that this menacing threat is the responsibility of the government alone.